REMARKS

The Examiner rejected claims 1-16 under 35 U.S.C. 112, first paragraph as failing to comply with the enablement requirement, stating that the claims contain subject matter that is not described in the specification in such a way as to enable one skilled in the art to which it pertains or with which it is most nearly connected to make and/or use the invention. Applicant respectfully traverses this rejection by the Examiner.

The Examiner states that at page 10, lines 12-17 it is not clear what the "times" are and how they are defined. As is apparent to one skilled in the art each of the "times" denotes a situation during the sequence of messages which is defined by the message immediately before and immediately after the situation, i.e., the occurrence of any new PDU in the sequence of messages causes a transition from one of these "times" to the next. Therefore the "times" are an arbitrary notation of the situation or interval between messages in the sequence of messages – the point between the first message and the second message of the sequence is assigned a "time" of "1", etc. It has no relationship to physical passage of time in terms of units of time, such as seconds. This is readily apparent from Fig. 5 when read in conjunction with the description at page 10. Thus each interval between messages is assigned a sequential "time."

The Examiner then states that it is not clear how the similarity matrix is established, i.e., the Examiner does not understand the description at page 11, lines 1-9. The entries into the similarity matrix, which relates two of the "times", is the sum of the lengths of the common prefix of PDU types and the common postfix of PDU types when comparing the PDU sequences surrounding the "times" in question. For example, where the capital letters indicate PDU types:

A t1 B t2 **B** t3 **A t4 C** t5 B t6 D t7 B t8 A t9 B t10 D t11 **B** t12 **A t13 C** t14 D t15 B t16 B

for times **t4** and **t13** the common prefix is BA (length 2), the common postfix is C (length 1), so the entry (4,13) of the similarity matrix is 2+1=**3**. Applicant submits that this is clear from the description when read in light of Fig. 6.

The Examiner does not understand the concept of learning the concept rules as described at pages 13-15. First Applicant has corrected the paragraph at the bottom of page 13 for clarity, as the translated English was not quite clear, to state that "the message attributes of the first PDU of type **a** are **v** and **w**, of the first PDU of type **b** is **x** and of the second PDU of type **a** are **y** and **z**." For learning the context rules the analyzer knows the number of attributes per PDU type in advance and how to extract their values. These attributes and how they are encoded in the PDUs are defined by the protocol standard document. The names **v, w, x, y, z** are arbitrary shorthands. The required information from the protocol standard in this example are that PDU type **a** carries two numeric attributes, and PDU type **b** carries one. These attributes are used by the protocol to implement its service (reference the ISO/OSI documents) – they are NOT data as provided by the user of the protocol or any higher layer in the protocol stack. The collection of the set of PDUs is defined by the window size, three PDUs per window in this example. From determining the finite automaton it is already known to which protocol states each of the times belongs, as every state is derived as an equivalence class of times. So for every occurrence of state **s** the three PDUs in the window subsequent to the time identified for state **s** are taken as a "training sample" for the occurrence of state **s**. All training samples collected for state **s** are then split according to the sequence of the three PDU types therein, yielding a certain number of occurrences of state **s** with three subsequent

PDUs of types (**a, b, a**). For all THESE occurrences of (**a, b, a**) after **s** there is a vector of the five attributes (**v, w, x, y, z**) as defined above. These 5-dimensional vectors are the training data used to extract context rules regarding the described kind of event in the protocol communication. The existence, meaning and extraction of attributes depend on the protocol syntax, as usually described in the protocol standard document.

Page 14, lines 14-21 provide a good description of what happens – the analyzer formulates an **OK** criterion based on the analysis of the training samples. In this illustration the **OK** criteria are x=w+1, y=v+1 and z=x. With respect to page 15, lines 9-18 **t** is just one of the components of all the attribute vectors as collected for a certain event, as described above. The phrase "**t** has the value 5 four times" means that there have been four feature vectors observed regarding the event in question with the attribute value 5 for attribute **t**. The specification has been amended for clarity to recite "*in* an example communication", the word "in" being required for grammatical correctness.

The terms "quotient", "width", "gaps" and "numerical intervals" deal with the identification of conspicuous clusters of attribute values, so the visualization is frequency of the observation of a certain feature value in the corresponding events over numerical feature value. A "gap" is an interval of feature values in which no observed feature values lie. An interval is a range of numbers, i.e., feature values in the present case. The conditions expressed by the **OK** criteria are basically interval selections, i.e., 5<=**t**<=15 selects the interval 5 . . . 15 for feature **t**, so the decision to be made is which interval borders are chosen for the criteria. This is done by choosing the lower and upper bound of the criterion interval such that the width (interval width – upper bound minus lower bound) of the candidate criterion interval

itself (quotient being a mathematical term for division) is as big as possible. A "clause" is one of the conjunctive **OK** criteria. The constitution of the training set is described above.

In summary the first step of the present invention – finite automaton identification – assigns states to the times between subsequent messages so that "similar" times later correspond to the same state. For this purpose a relation (http://mathworld.wolfram.com/Relation.html) is defined to formalize "similarity" as described in the specification and above. Then the similarity relationship is transformed into an equivalence relation (http://mathworld.wolfram.com/EquivalenceRelation.html) which uniquely defines equivalence classes (http://mathworld.wolfram.com/EquivalenceClass.html) within the set of times in the observed communication. Each of these equivalence classes yields a state of the derived finite automaton of the protocol. The transformation from the similarity relation to the equivalence relation is described in the specification and above – it is necessary to fulfill the "transitive" property which the similarity relation does not generally have (if A, B are in the same class and B, C are in the same class, then A and C obviously have to be in the same class as well).

In light of the above discussion it is submitted that the specification provides sufficient description of the subject matter recited in the claims to enable one of ordinary skill in the art to practice the invention. Thus claims 1-16 are deemed to be allowable as being supported by an enabling specification.

The Examiner rejected claim 1-16 also under 35 U.S.C. 112, second paragraph as being indefinite. Particularly in claim 1 the Examiner states it is not clear what is meant by "grouping times . . . as equivalent classes." Based upon the above discussion it should be clear to one of ordinary skill in the art who has read the specification what this claim element means – an example communication is a

sequence of messages where the times identify sequential intervals or situations between messages and are grouped as discussed above to form equivalence classes. Likewise the claim 2 element "calculating a similarity value between every two times within the example communication to form a similarity matrix, the similarity values being dependent on the length of the PDU type sequence which is coincident for and surrounds both times" is adequately described in the specification, as discussed above. Therefore claims 1 and 2 are deemed to be definite as particularly pointing out and distinctly claiming what Applicant regards as the invention for one of ordinary skill in the art who has read the specification.

In the event there is some misunderstanding regarding the Declaration filed by the Inventor due to the poor printing of the form, Applicant is claiming priority from German Application No. 199 29 166.7 filed June 25, 1999 and from EPO Application No. 00 11 00 67.6 filed May 12, 2000.

In view of the foregoing amendment and remarks allowance of claims 1-16 is urged, and such action and the issuance of this case are requested.

Respectfully submitted,

MAREK MUSIAL

TEKTRONIX, INC.
P.O. Box 500 (50-LAW)
Beaverton, OR 97077
(503) 627-7261

By Francis I. Gray

Francis I. Gray
Reg. No. 27,788
Attorney for Applicant

6963 US